

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
By: Jerry Fang / Danielle Kudla
Assistant United States Attorneys
26 Federal Plaza
New York, New York 10278
Tel: (212) 637-2584 / 2304

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

- v. -

ALL ASSETS FORMERLY CONTAINED IN
CERTAIN BINANCE ACCOUNTS SEIZED BY
THE GOVERNMENT ON OR ABOUT
FEBRUARY 15, 2022 AND ALL FUNDS
TRACEABLE THERETO TO EACH LISTED
ACCOUNT, INCLUDING ACCRUED INTEREST

Defendants-*in-rem*.

**VERIFIED CIVIL
COMPLAINT FOR
FORFEITURE**

24 Civ. 3894

Plaintiff United States of America, by its attorney, Damian Williams, United States Attorney for the Southern District of New York, for its verified civil complaint, alleges, upon information and belief, as follows:

JURISDICTION AND VENUE

1. This action is brought pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 981(a)(1)(C) by the United States of America seeking the forfeiture of the following:

All assets and funds formerly contained in certain Binance accounts as specifically described in Exhibit A (the “Defendants-*in-rem*”) attached hereto that were seized by the Government on or about February 15, 2022 from the following accounts:

- a. BINANCE ACCOUNT ID 77119125 (“Account-1”);
- b. BINANCE ACCOUNT ID 126431418 (“Account-2”);
- c. BINANCE ACCOUNT ID 177870794 (“Account-3”);
- d. BINANCE ACCOUNT ID 46381766 (“Account-4”);
- e. BINANCE ACCOUNT ID 184735647 (“Account-5”);
- f. BINANCE ACCOUNT ID 89843434 (“Account-6”);
- g. BINANCE ACCOUNT ID 90063455 (“Account-7”);
- h. BINANCE ACCOUNT ID 110720525 (“Account-8”);
- i. BINANCE ACCOUNT ID 38246708 (“Account-9”);
- j. BINANCE ACCOUNT ID 10851856 (“Account-10”);
- k. BINANCE ACCOUNT ID 214062148 (“Account-11”);
- l. BINANCE ACCOUNT ID 37112946 (“Account-12”);
- m. BINANCE ACCOUNT ID 66161377 (“Account-13”);
- n. BINANCE ACCOUNT ID 166730652 (“Account-14”);
- o. BINANCE ACCOUNT ID 10876619 (“Account-15”);
- p. BINANCE ACCOUNT ID 145203723 (“Account-16”);
- q. BINANCE ACCOUNT ID 40782626 (“Account-17”);
- r. BINANCE ACCOUNT ID 64959391 (“Account-18”);
- s. BINANCE ACCOUNT ID 37516098 (“Account-19”);
- t. BINANCE ACCOUNT ID 113476746 (“Account-20”);

- u. BINANCE ACCOUNT ID 91345082 (“Account-21”);
- v. BINANCE ACCOUNT ID 41226929 (“Account-22”);
- w. BINANCE ACCOUNT ID 56577372 (“Account-23”); and
- x. BINANCE ACCOUNT ID 148017544 (“Account-24”);

(collectively, the “Subject Accounts”).

2. This Court has original jurisdiction over this forfeiture action pursuant to Title 28, United States Code, Sections 1345 and 1355.

3. Venue is proper pursuant to Title 28, United States Code, Section 1395 because the Defendants-*in-rem* are currently held in the Seized Asset Deposit Fund Account of the United States Marshals Service (the “USMS”) located within the judicial district for the Southern District of New York. Venue is also proper pursuant to Title 28, United States Code, Section 1355(b)(1)(A) because the acts and omissions giving rise to the forfeiture took place in the Southern District of New York and elsewhere.

4. As set forth below, there is probable cause to believe that the Defendants-*in-rem* are subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) as proceeds traceable to wire fraud, in violation of Title 18, United States Code, Section 1343, or property traceable thereto; and pursuant to Title 18, United States Code, Sections 981(a)(1)(A) as property involved in money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957.

FACTUAL ALLEGATIONS

5. This action arises out of an investigation conducted by the Federal Bureau of Investigation (“FBI”) and Special Agents with the United States Attorney’s Office of the Southern District of New York (“USAO-SDNY”) into a business email compromise (“BEC”) and

romance fraud and money laundering scheme that began at least in February 2021 and lasted until at least September 2021.

6. Specifically, in or around February 2021, investigators learned that a woman (the “Victim”) met an individual online who asked to be called “Eddie Hernandez” (the “Subject”) and portrayed himself as the Victim’s romantic partner. At the Subject’s direction, the Victim opened business and personal bank accounts, which received nearly \$10 million from a real estate company located during the relevant time in Santa Ana, California (“Business Victim-1”) and a medical/pharmaceutical company located during the relevant time in Manhattan, New York, which had a subsidiary located during the relevant time in Scottsdale, Arizona (“Business Victim-2” and collectively, the “Business Victims”) that incorrectly believed that they were paying legitimate vendor invoices.

7. In reality, certain email accounts for the Business Victims and/or email accounts for parties trusted by the Business Victims were compromised by members of the fraud conspiracy. Once compromised, the email accounts were used to send email messages that instructed the Business Victims to wire future invoice payments to business bank accounts that had been established by the Victim at the Subject’s direction.

8. After the Victim received the Business Victims’ funds (the “Fraud Proceeds”), the Victim transferred the Fraud Proceeds to personal bank accounts and then to a particular cryptocurrency exchange account at the Subject’s direction.

9. Ultimately, the Victim was instructed by the Subject to use the Fraud Proceeds to purchase cryptocurrency and transfer the cryptocurrency to various cryptocurrency addresses, approximately half of which has been traced to the Subject Accounts.

10. As part of the investigation, on or about February 15, 2022, the Honorable

Sarah L. Cave, United States Magistrate Judge for the Southern District of New York, issued a seizure warrant captioned 22 Mag. 1572 for the Subject Accounts (the “Seizure Warrant”), authorizing the seizure of all assets and funds contained in the Subject Accounts, and all funds traceable thereto to each listed account, including accrued interest, upon a finding that the Subject Accounts contain funds representing proceeds traceable to and/or property involved in the money laundering, romance and BEC schemes. A copy of the Seizure Warrant and its supporting materials is attached hereto as Exhibit B, and is incorporated by reference as if set forth fully herein.

THE ROMANCE FRAUD

11. As set forth in greater detail in the Seizure Warrant, in or about February 2021, the Victim met the Subject via an online dating application.

12. The Subject described himself, in substance and in part, as an individual working for the United Nations in Venezuela who owned a medical company that was assisting with the country’s COVID-19 outbreak. The Subject falsely claimed that he owned companies in the United States and needed the Victim’s assistance transferring money from these companies. The Subject also falsely claimed that the money would be used to purchase medical supplies. To assist, the Subject directed the Victim to take the following actions:

a. In or about April 2021, the Subject directed the Victim to register Hernandez Medical Supplies, LLC (“Hernandez Medical Supplies”) as a business entity with the North Dakota Secretary of State.

b. From in or about April 2021 through in or about June 2021, the Subject directed the Victim to open two business accounts for Hernandez Medical Supplies at two different financial institutions, Wells Fargo (the “Wells Fargo Business Account”) and Bank of

America (the “BofA Business Account” and collectively, the “Business Accounts”), along with two personal accounts in the Victim’s name at each bank (the “Wells Fargo Personal Account” and the “BofA Personal Account” and collectively, the “Personal Accounts”). The Subject directed the Victim to link the Business Accounts to the Personal Accounts at each respective bank.

c. In or about July 2021, the Subject also directed the Victim to open a Binance cryptocurrency account (the “Binance Account”) in the Victim’s name. Binance is a cryptocurrency exchange that allows customers to trade cryptocurrencies for other assets, such as conventional fiat money or other digital currencies. The Binance Account was linked to the BofA and Wells Fargo Personal Accounts. Between the Binance Account creation and approximately in or about October 2021, the Subject (along with the Victim) had access to and control of the Binance Account.

d. In or about July 2021, the Subject asked the Victim to transfer money on his behalf, which the Subject falsely said would be used to purchase medical supplies in Venezuela. At the Subject’s direction, the Victim transferred approximately \$170,000 that had been deposited into the BofA Business Account by Business Victim-1, as described in greater detail in paragraph 15 *infra*, from the BofA Business Account to the BofA Personal Account, and then to the Binance Account.

e. In or about September 2021, the Subject asked the Victim to transfer additional money on his behalf. At the Subject’s direction, the Victim transferred approximately \$9.5 million that had been deposited into the Wells Fargo Business Account by Business Victim-2,

as described in greater detail in paragraph 16 *infra*, from the Wells Fargo Business Account to the Wells Fargo Personal Account, and then to the Binance Account through a series of transactions.

f. Each time the Victim transferred funds to the Binance Account at the Subject's direction, the Subject also instructed the Victim to purchase Bitcoin, a particular cryptocurrency, with the transferred funds. Thereafter, the Subject directed the Victim to transfer the Bitcoin to approximately 12 different cryptocurrency addresses (the "Original Cryptocurrency Addresses"). The Victim did not have access to or control of the Original Cryptocurrency Addresses.

13. In or about late September 2021, the Victim was notified by Wells Fargo of suspected fraud activity. When the Victim confronted the Subject about the fraud allegations, the Subject discontinued communication with the Victim.

THE BUSINESS EMAIL COMPROMISE ("BEC") FRAUD

14. Business Victim-1 is a real estate company located during the relevant time in Santa Ana, California, and Business Victim-2 is a medical/pharmaceutical company located during the relevant time in Manhattan, New York, with a subsidiary located during the relevant time in Scottsdale, Arizona.

15. According to representatives and records obtained from Business Victim-1, investigators learned, among other things, the following:

a. In or about early July 2021, a Business Victim-1 employee received an email, which appeared to have been sent from a legitimate Business Victim-1 vendor, instructing Business Victim-1 to send an outstanding invoice payment by wire transfer to a specific account (the "July 2021 Email").

b. In accordance with the July 2021 Email instructions, Business

Victim-1 wired approximately \$171,535 to the BofA Business Account.

c. In or about October 2021, Business Victim-1 learned that the July 2021 Email was fraudulent when Business Victim-1 received a call from the legitimate Business Victim-1 vendor regarding the outstanding invoice balance.

16. According to representatives and business records of Business Victim-2, investigators learned, among other things, the following:

a. In or about August 2021, Business Victim-2 received an email, which appeared to have been sent from a legitimate Business Victim-2 employee to Business Victim-2's accounts payable department (the "August 2021 Email"). The August 2021 Email instructed Business Victim-2's accounts payable department to change the wiring instructions for a particular legitimate Business Victim-2 vendor.

b. Between on or about September 1, 2021 and on or about September 15, 2021, Business Victim-2 wired approximately \$9,540,139.78 in a series of wire transactions to the Wells Fargo Business Account.

c. In or about October 2021, Business Victim-2 learned that the August 2021 Email was fraudulent when the legitimate Business Victim-2 vendor reported that it did not receive the transferred funds.

17. Records obtained during the course of the investigation revealed the following, among other things:

a. On or about July 28, 2021, Business Victim-1 transferred approximately \$171,535 to the BofA Business Account. On or about July 28, 2021, approximately \$171,541.73 was transferred from the BofA Business Account to the BofA Personal Account by the Victim, at the Subject's direction. On or about July 29, 2021, approximately \$170,000 was

transferred from the BofA Personal Account to the Binance Account by the Victim, at the Subject's direction. On or about July 29, 2021, and on or about August 24, 2021, approximately 4.26812659 Bitcoin, then-valued at approximately \$188,610.751, was purchased and transferred from the Binance Account to two of the Original Cryptocurrency Addresses by the Victim, all at the Subject's direction.

b. Between on or about September 1, 2021 and on or about September 17, 2021, Business Victim-2 transferred approximately \$9,540,139.78 to the Wells Fargo Business Account in a series of approximately four wire transactions. Between on or about September 1, 2021, and on or about September 21, 2021, approximately \$9,523,500 was transferred from the Wells Fargo Business Account to the Wells Fargo Personal Account by the Victim, at the Subject's direction. Between the same period, approximately \$9,519,000 was transferred from the Wells Fargo Personal Account to the Binance Account by the Victim, at the Subject's direction. Between the same period, approximately 205.1196697 Bitcoin, then-valued at approximately \$9,467,485, was purchased and transferred from the Binance Account in various amounts to ten of the Original Cryptocurrency Addresses by the Victim, all at the Subject's direction.

THE DEFENDANTS-IN-REM

18. Cryptocurrency is any currency, money, or money-like asset that is primarily managed, stored, and/or exchanged on digital computer systems. Cryptocurrency is a decentralized, peer-to-peer form of electronic currency that has no association with banks or governments. Like traditional fiat currency, there are multiple types of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, and Tether, among others. Due to its decentralized nature and limited regulation, cryptocurrency allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. Although they are legal and have known

legitimate uses, cryptocurrency is also known to be used by cybercriminals for money-laundering purposes.

19. Cryptocurrency owners typically store their cryptocurrency in digital “wallets,” which are identified by unique electronic “addresses.” By maintaining multiple cryptocurrency addresses, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track the flow of illegal proceeds by quickly transferring illicit proceeds in various amounts through multiple cryptocurrency addresses.

20. Each cryptocurrency transaction, however, regardless of the cryptocurrency denomination, is recorded on a public database commonly referred to as the “blockchain,” which acts as an accounting ledger. The blockchain records, among other things, the date and time of each cryptocurrency transaction, the unique cryptocurrency addresses associated with the sending and receiving parties, and the amount of cryptocurrency transferred. Because each cryptocurrency address is unique, law enforcement can review the blockchain to identify relevant cryptocurrency transactions and trace the flow of cryptocurrency across various cryptocurrency addresses. This form of cryptocurrency tracing is labor intensive and complicated by each transfer to a different cryptocurrency address.

21. According to Binance records, and the blockchain public ledger, it appears that the Original Cryptocurrency Addresses were used to transfer approximately 209.3877963 Bitcoin, then-valued at approximately \$9,468,602, in more than 150 separate transactions across numerous cryptocurrency addresses in quick, back-to-back transactions.

22. Within days after their initial transfers from one of the Original Cryptocurrency Addresses, approximately 104.3853109 Bitcoin, representing approximately half of the Fraud Proceeds, were deposited into the Subject Accounts. Specifically, each of the Subject

Accounts received the following approximate Bitcoin amounts traceable to the Fraud Proceeds:

- *Account-1*: 0.38407565 Bitcoin;
- *Account-2*: 0.09247806 Bitcoin;
- *Account-3*: 0.02330937 Bitcoin;
- *Account-4*: 0.04584544 Bitcoin;
- *Account-5*: 5.64188902 Bitcoin;
- *Account-6*: 10.0903650 Bitcoin;
- *Account-7*: 0.08328527 Bitcoin;
- *Account-8*: 0.66875044 Bitcoin;
- *Account-9*: 0.00759616 Bitcoin;
- *Account-10*: 0.00516007 Bitcoin;
- *Account-11*: 35.35763078 Bitcoin;
- *Account-12*: 0.01574103 Bitcoin;
- *Account-13*: 0.08875962 Bitcoin;
- *Account-14*: 0.07602 Bitcoin;
- *Account-15*: 0.11185449 Bitcoin;
- *Account-16*: 2.33767565 Bitcoin;
- *Account-17*: 0.06464140 Bitcoin;
- *Account-18*: 0.05449369 Bitcoin;
- *Account-19*: 1.36093099 Bitcoin;
- *Account-20*: 46.92552132 Bitcoin;
- *Account-21*: 0.04200274 Bitcoin;
- *Account-22*: 0.0582625 Bitcoin;
- *Account-23*: 0.17978881 Bitcoin; and

- *Account-24*: 0.6792333 Bitcoin

23. In total, the Subject Accounts received approximately 104.3853109 Bitcoin in Fraud Proceeds, which, as of February 15, 2022, was valued at approximately \$4,608,058.23.

24. Based on the foregoing, the Defendants-*in-rem* are subject to forfeiture, pursuant to 18 U.S.C. § 981(a)(1)(A), as they constitute property involved in money laundering of the Fraud Proceeds as demonstrated by the multiple deposits of various cryptocurrency amounts over a short period, and pursuant to 18 U.S.C. § 981(a)(1)(C), as they constitute property constituting or derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or property traceable to such property. The series of quick, back-to-back cryptocurrency transactions, many of which ultimately resulted in approximately half of the Fraud Proceeds being deposited into the Defendants-*in-rem*, is an effort to maintain digital anonymity and launder the Fraud Proceeds, which were obtained through fraudulent means.

CLAIMS FOR FORFEITURE

Forfeiture Under 18 U.S.C. § 981(a)(1)(A) (Property Involved in a Transaction or Attempted Transaction in Violation of 18 U.S.C. § 1956 or Property Traceable to Such Property)

25. Paragraphs 1 through 24 of this Complaint are repeated and re-alleged as if fully set forth herein.

26. Pursuant to Title 18, United States Code, Section 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of Title 18, United States Code, Section 1956, or any property traceable to such property, is subject to forfeiture to the United States.

27. Title 18, United States Code, Section 1956(a)(1)(A)(i) & (a)(1)(B)(i) imposes a criminal penalty on any person who:

knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity . . .

- (A) (i) with the intent to promote the carrying on of specified unlawful activity; . . . or
- (B) knowing that the transaction is designed in whole or in part . . . (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity[.]

28. As defined in Title 18, United States Code, Section 1956(c)(7), “specified unlawful activity” includes, among other things, racketeering activity as defined in 18 U.S.C. § 1961(1). Section 1961(1), in turn, defines racketeering activity to include wire fraud, in violation of 18 U.S.C. § 1343.

29. Title 18, United States Code, Section 1343 provides, in relevant part:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

30. By reason of the foregoing, the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(A) as property involved in a money laundering transaction or an attempted money laundering transaction, in violation of Title 18, United States Code, Section 1956, or as property traceable to such property.

**Forfeiture Under 18 U.S.C. § 981(a)(1)(A)
(Property Involved in a Transaction or Attempted Transaction in Violation of 18 U.S.C.
§ 1957 or Property Traceable to Such Property)**

31. Paragraphs 1 through 30 of this Complaint are repeated and re-alleged as if fully set forth herein.

32. Pursuant to Title 18, United States Code, Section 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of Title 18, United States Code, Section 1957, or any property traceable to such property, is subject to forfeiture to the United States.

33. Title 18, United States Code, Section 1957 imposes a criminal penalty on any person who “knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity.” Section 1957(f)(1) defines “monetary transaction” to include the “deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds”

34. Section 1957(f)(3) defines “specified unlawful activity” to have the same meaning as given in Section 1956. As set forth above, wire fraud, in violation of Title 18, United States Code, Section 1343, is a specified unlawful activity for purposes of Section 1956.

35. By reason of the foregoing, the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(A) as property involved in a money laundering transaction or an attempted money laundering transaction, in violation of Title 18, United States Code, Section 1957, or as property traceable to such property.

**Forfeiture Under 18 U.S.C. § 981(a)(1)(C)
(Property Constituting or Derived from Proceeds Traceable to a Violation of 18 U.S.C.
§ 1343 or Property Traceable to Such Property)**

36. Paragraphs 1 through 35 of this Complaint are repeated and re-alleged as if fully set forth herein.

37. Pursuant to Title 18, United States Code Section 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of any

offense constituting “specified unlawful activity” as defined in section 1956(c)(7) of this title, or a conspiracy to commit such offense.

38. As set forth above, for purposes of Section 1956, “specified unlawful activity” includes wire fraud, in violation of Title 18, United States Code, Section 1343.

39. By reason of the foregoing, the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) as property constituting or derived from proceeds traceable to a violation of Title 18, United States Code, Section 1343.

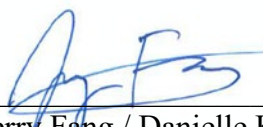
CONCLUSION

WHEREFORE, plaintiff United States of America prays that process issue to enforce the forfeiture of the Defendants-*in-rem* and that all persons having an interest in the Defendants-*in-rem* be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the Defendants-*in-rem* to the United States of America for disposition according to law, and that this Court grant plaintiff such further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: New York, New York
May 20, 2024

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
Attorney for the Plaintiff
United States of America

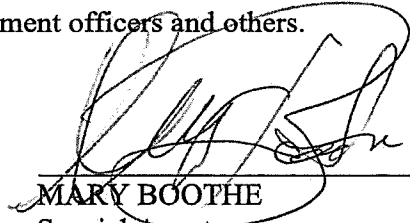
By: _____


Jerry Fang / Danielle Kudla
Assistant United States Attorneys
26 Federal Plaza, 37th Floor
New York, New York 10278
Telephone: (212) 637-2584 / 2304

DECLARATION OF VERIFICATION

MARY BOOTHE, pursuant to Title 28, United States Code, Section 1746, hereby declares under penalty of perjury that she is a Special Agent with the Federal Bureau of Investigation; that she has read the foregoing Verified Complaint and knows the contents thereof; that the same is true to the best of her knowledge, information and belief; and that the sources of her information and the grounds of her belief are her personal involvement in the investigation, and conversations with and documents prepared by law enforcement officers and others.

Executed on May 20, 2024



MARY BOOTHE
Special Agent
Federal Bureau of Investigation